Authentication Beyond Desktops and Smartphones: Novel Approaches for Smart Devices and Environments

Stefan Schneegass
University of Duisburg-Essen
stefan.schneegass@uni-due.de

Florian Alt
Bundeswehr University Munich
florian.alt@unibw.de

Angela Sasse
Ruhr University Bochum
martina.sasse@ruhr-uni-bochum.de

Daniel Vogel
University of Waterloo
dvogel@uwaterloo.ca

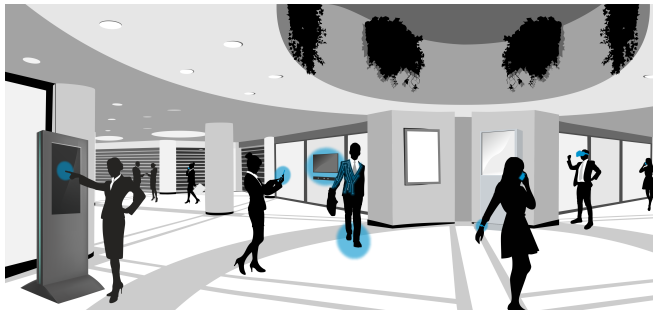

Figure 1: This workshop identifies challenges and future research directions for authentication in smart devices and environments.

CHI'20 Extended Abstracts, April 25–30, 2020, Honolulu, HI, USA
ACM 978-1-4503-6819-3/20/04.
https://doi.org/10.1145/3334480.3375144

Abstract
Much of the research on authentication in the past decades focused on developing authentication mechanisms for desktop computers and smartphones with the goal of making them both secure and usable. At the same time, the increasing number of smart devices that are becoming part of our everyday life creates new challenges for authentication, in particular since many of those devices are not designed and developed with authentication in mind. Examples include but are not limited to wearables, AR and VR glasses, devices in smart homes, and public displays. The goal of this workshop is to develop a common understanding of challenges and opportunities smart devices and environments create for secure and usable authentication. Therefore, we will bring together researchers and practitioners from HCI, usable security, and specific application areas (e.g., smart homes, wearables) to develop a research agenda for future approaches to authentication.

Author Keywords
Authentication; Ubicomp; Smart Environments

CCS Concepts
•Security and privacy → Usability in security and privacy; •Human-centered computing → Human computer interaction (HCI);

Introduction

The quick proliferation of our daily life with new technology in the past decade has fuelled the need to rethink the way in which we design security mechanisms, in particular authentication. Such technology allows for *collecting sensitive data* about the user as well as to *access sensitive data* stored in the cloud. Examples include but are not limited to smart watches, smart glasses, smart home devices (coffee machines, cleaning robots), smart speakers, head-mounted AR&VR displays, and public displays (cf., Figure 1).

What is striking is that the vast majority of smart devices are designed without adhering to fundamental privacy and security needs, such as encryption or authentication. This often creates a need to add security means post-hoc, for example, a smart phone app or a remote control that enables secure access to the configuration of, or data collected by, a smart home device. Such workarounds – i.e. using external input and output devices – usually comes at the expense of good usability. This may ultimately lead to users trading low security for high usability, for example, not using means for security at all; or minimizing the required effort by reusing short and easy-to-remember passwords.

Beyond data collection and enabling secure information access, novel technologies also not only create *new threats* – for example, attack models based on ubiquitously available high-resolution cameras or thermal imaging [1] – but also *opportunities* – for example, novel sensor-based authentication mechanisms exploiting behavioural cues. Hence, authentication mechanisms that do not require any user action and blend with the way in which people use technology today become feasible [3]. Another opportunity is the ability to design mechanisms that adjust to the current context. For example, a higher level of security might be required as users access sensitive data in public compared to at home.

In this workshop, we will bring together people who investigate novel means of identifying and authenticating users in smart environments and on smart devices. In particular, we focus on the challenge of providing secure yet usable authentication [2]. The CHI community provided first examples of such systems in the last years. This includes research on biometrics using the body shape of users [7] or body reflections generated through audio stimuli [11]. Behavioral data has been used, for example, to authenticate users of virtual reality headsets [10] as well as on smart phones [4, 5, 8].

The main objective of this workshop is to identify fundamental research challenges for authentication on smart devices and in smart environments – this includes ethical, societal, and technical challenges – as well as to develop a research agenda that will help the community to address the identifies challenges in the future with the goal of designing appropriate authentication mechanisms for smart environments. We plan to disseminate the outcomes of the workshop in the form of a special issues on future authentication approaches.

Key Questions for the Workshop

The following key questions will form the basis for discussions at the workshop.

Limited Input and Output Capabilities

Many smart devices are not designed with appropriate input and output capabilities for authentication. Rather such means are added post-hoc or other devices are used as substitute (e.g., using a smartphone to control devices in a smart home). This often leads to both poor usability and security. One fundamental question is here how to support considering the integration of means for protecting and enabling access to sensitive information for smart devices early in the design process.

Concerns and Communication
The fact that in smart environments data about the user is available from personal devices and sensors in the environment enables novel means for authentication. This includes biometric approaches, leveraging users' physiology (fingerprint, face, iris, body parts) or behavior (gait, typing, touch targeting). This creates a need to understand general concerns of users towards such authentication mechanisms, in particular since it is often not clear which data is collected, how and where it is processed, what is stored, and who has access to it. From an HCI perspective, an important question is how to communicate this information to the user.

Scalability of Behavioural Biometrics
Behavioral biometrics is one approach that has received considerable attention in the past years. While much of the research so far has been conducted in the lab, mainly with the goal of understanding of how accurately different behavior traits allow for identifying the user, it is an open question what challenges emerge as this technology becomes widely used. Possible questions include: How does the authentication context influence user behavior? How can appropriate re-authentication mechanisms be designed?

Contextual Authentication Mechanisms
A major challenge of current authentication mechanisms is that they often do not consider the context in which they are used. For example, smartphones employ the same means for authentication, independent of the presence of potential adversaries. This creates a large authentication overhead, i.e. Harbach et al. showed that the average smartphone user spends about 1.5 hours every month authenticating [6]. One core question we will discuss at the workshop is how we can design authentication mechanisms that better account for the context in which they are used to substantially increase their usability.

Research Approaches
Designing novel approaches to authentication in smart environments requires new research methods. We will discuss appropriate methods to assess requirements (e.g., data collection methods) as well as to evaluate novel approaches regarding usability, security, UX, and acceptance.

Novel Thread Models
Novel authentication approaches also provides new opportunities for attackers. For example, the use of people's behavior as a means for authentication allows attackers to get access to a system by mimicking a legitimate user's behavior [8, 9]. We will identify such novel threat models and discuss how they can be mitigated.

Topics of Interest
In this workshop we will solicit submissions that cover a broad range of topics related to the overall theme. In particular, we are interested in work that addresses one of the following topics:

- Novel authentication concepts for smart environments
- User requirements for authentication systems
- Physiological and behavioral biometrics
- Authentication in specific application areas (e.g., smart home, smart public spaces)
- Novel thread models
- Users' experience of authentication systems
- Privacy in smart environments
- Challenges of implicit authentication systems
- Novel methodologies for evaluating authentication systems
- Evaluation of authentication systems in the large
- Ethical and societal implications of novel authentication systems

Time	Activity
9:00-9:10	Opening & Introduction
9:10-10:30	Presentation of the selected submissions
10:30-12:30	Poster session (incl. coffee break)
12:30-14:00	Lunch
14:00-16:00	Creating concepts for novel authentication systems (incl. coffee break)
16:00-17:00	Breakout session on future research agenda
17:00-17:30	Wrap-up and discussion on follow-up activities

Table 1: Planned workshop schedule.

Workshop Structure

Table 1 shows a detailed schedule of the workshop. In the first half of the workshop, participants will present their position papers. We will select the most inspiring papers to be presented as talks whereas the other papers will be presented in an interactive, 90-minute poster session.

The afternoon will be spent with group activities in which we will foster active communication among participants. In particular, we will first focus on generating novel concepts for authentication mechanisms in smart environments and with smart devices. The outcome of this session will form the basis of a follow-up breakout session in the context of which we will derive a future research agenda. The workshop will conclude with a wrap-up and discussing follow-up activities.

Website & Social Media

We will provide a website[1] and create social media accounts (e.g., Facebook) to advertise the workshop and to foster communication between participants prior to and after the workshop.

[1] Website will be created upon acceptance: https://www.hcigroup.de/authenticationworkshop

Date	Action
1st December	Release of the Webpage, release of the Call for Participation & selection of program committee
11th February	Submission Deadline
28th February	Notification of Acceptance
25th/26th	Workshop at CHI 2020

Table 2: Important workshop dates.

Furthermore, we will provide all important information on the website, including a link to the submission system as well as important references to allow participants to gain a mutual understanding of the workshop theme prior to the event. Papers will also be published on the website.

During the workshop we will create a shared document to collect all information generated throughout the workshop (minutes of discussions, presentations, mindmaps, etc.) and made available to all participants after the workshop.

Pre-Workshop Plans

We intend a workshop size of about 20 participants. Prior to the workshop, we will advertise the workshop and solicit submissions through social media and mailing lists. To attract people to the workshop we will put together a small program committee of well-known experts in related areas.

Workshop participants hand in position papers of up to 4 pages in the ACM SIGCHI Extended Abstract format. Papers should contribute the authors' opinion on the workshop theme but also provide specific ideas for work on future authentication or work addressing a related research question. The submission of position papers will be handled through a conference management system. The program committee will review all submissions.

Post-Workshop Plans

We plan to disseminate the outcomes of the workshop in the form of a special issue on authentication with smart devices and in smart environments. To do so, we will discuss with the participants two ways of contributing to this special issue. First, we will encourage participants to extend their position papers to potential submission for this issue. Second, we will encourage the participant to build on ideas generated in the workshop.

Organizers

Stefan Schneegass

Stefan Schneegass is an Assistant Professor of human-computer interaction at the University of Duisburg-Essen. He is interested in researching the crossroad of human-computer interaction and ubiquitous computing. Thereby, one core focus of his current research is the development of implicit authentication mechanisms. He organized several workshops at conferences such as CHI and Ubicomp.

Florian Alt

Florian Alt is a Professor of Usable Security and Privacy at the Research Institute CODE of the Bundeswehr University in Munich. In his research, Florian looks at the role of humans in security critical systems, focusing on topics related to behavioral biometrics, physiological security, social engineering and usable security in novel application areas, such as smart homes and VR. He has organized workshops on various topics at the intersection of HCI and Ubicomp. He is the workshop chair of ACM ETRA 2020.

Angela Sasse

M. Angela Sasse is the Professor of Human-Centred Security at the Horst Görtz Institute at Ruhr University Bochum in Germany. She also retains a part-time appointment as professor at in the Department of Computer Science at University College London, UK. A usability researcher by training, she started investigating the causes and effects of usability issues with security mechanisms in 1996. In addition to studying specific mechanisms such as passwords, biometrics, and access control, her research group has developed human-centred frameworks that explain the role of security, privacy, identity and trust in human interactions with technology.

Daniel Vogel

Daniel Vogel is an Associate Professor in the Cheriton School of Computer Science at the University of Waterloo. His research focuses on fundamental characteristics of human input and novel forms of interaction for current and future computing form factors like touch, tangibles, large displays, mid-air gestures, and whole-body input. In addition to earning PhD and MSc degrees from the University of Toronto, Dan holds a BFA from the Emily Carr University of Art + Design, and he leverages his combined art and science background in his research.

Conclusion

Providing secure yet usable authentication mechanisms is a core challenge for smart devices and environments. In this workshop we will bring together experts to gain a common understanding of the challenges and work on potential solutions.

Acknowledgements

The presented work was funded by the German Research Foundation (DFG) under project no. 425869382.

REFERENCES

[1] Yomna Abdelrahman, Mohamed Khamis, Stefan Schneegass, and Florian Alt. 2017. Stay Cool! Understanding Thermal Attacks on Mobile-based User

Authentication. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. ACM, New York, NY, USA, 3751–3763.

[2] Anne Adams and Martina Angela Sasse. 1999. Users are not the enemy. *Commun. ACM* 42, 12 (1999), 41–46.

[3] A. Alzubaidi and J. Kalita. 2016. Authentication of Smartphone Users Using Behavioral Biometrics. *IEEE Communications Surveys Tutorials* 18, 3 (thirdquarter 2016), 1998–2026.

[4] Daniel Buschek, Alexander De Luca, and Florian Alt. 2015. Improving Accuracy, Applicability and Usability of Keystroke Biometrics on Mobile Touchscreen Devices. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15)*. ACM, New York, NY, USA, 1393–1402.

[5] Daniel Buschek, Alexander De Luca, and Florian Alt. 2016. Evaluating the Influence of Targets and Hand Postures on Touch-based Behavioural Biometrics. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16)*. ACM, New York, NY, USA, 1349–1361.

[6] Marian Harbach, Emanuel Von Zezschwitz, Andreas Fichtner, Alexander De Luca, and Matthew Smith. 2014. It's a Hard Lock Life: A Field Study of Smartphone (Un)Locking Behavior and Risk Perception. In *Proceedings of the Tenth USENIX Conference on Usable Privacy and Security (SOUPS '14)*. USENIX Association, Berkeley, CA, USA, 213–230.

[7] Christian Holz, Senaka Buthpitiya, and Marius Knaust. 2015. Bodyprint: Biometric User Identification on Mobile Devices Using the Capacitive Touchscreen to Scan Body Parts. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15)*. ACM, New York, NY, USA, 3011–3014.

[8] Hassan Khan, Urs Hengartner, and Daniel Vogel. 2018. Augmented Reality-based Mimicry Attacks on Behaviour-Based Smartphone Authentication. In *Proceedings of the 16th Annual International Conference on Mobile Systems, Applications, and Services (MobiSys '18)*. ACM, New York, NY, USA, 41–53.

[9] Lukas Mecke, Daniel Buschek, Mathias Kiermeier, Sarah Prange, and Florian Alt. 2019. Exploring intentional behaviour modifications for password typing on mobile touchscreen devices. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*.

[10] Ken Pfeuffer, Matthias J. Geiger, Sarah Prange, Lukas Mecke, Daniel Buschek, and Florian Alt. 2019. Behavioural Biometrics in VR: Identifying People from Body Motion and Relations in Virtual Reality. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19)*. ACM, New York, NY, USA, Article 110, 12 pages.

[11] Stefan Schneegass, Youssef Oualil, and Andreas Bulling. 2016. SkullConduct: Biometric User Identification on Eyewear Computers Using Bone Conduction Through the Skull. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16)*. ACM, New York, NY, USA, 1379–1384.